

used by others with or without permission, borrowed and so forth. I can call my ISP and they can willfully take control of my computer and fix it or just review it to see if I am infected. I did this with Centurytel about fifteen years ago over the telephone. Most people believe they actually control their computer when nothing could be further from the truth. The point here is not to blame Defendants for things which may have happened on their computer since these used machines are already filled with torrents, used by innocent children, spoofed and hacked by neighbors, drive byes or anyone connected to the internet. Many internet scams take control of your computer after a user sees a threatening pop up, calls the scammer who claims to be able to fix your computer, transfers control to the scammer who often puts a real virus into your computer, and then the scammer charges a fee to the user who often does not realize they have been scammed.

Regarding IP addresses and the Plaintiff's tracking method. Firstly, IP addresses are shared and exist throughout the entire world in the billions. Internet users are differentiated via identical and reusable IP addresses because of being acquired at different times and noted as such. The IP addresses are only as good as their source which is often manipulated, created for a small fee, wrongly identified as to its' rightful owner, placed into a homemade, Comcast, or store bought Excel box and then introduced by the Plaintiff as evidence of infringement. It is frightfully becoming child's play just like joining Al-Qaeda over the internet, having a phony girlfriend or boyfriend relationship that is Cyber space driven, creating false news stories or making movies with long dead actors and positioning them into current movies and of course, photo shopping camera pictures. Nobody knows what they are looking at anymore and especially who created it.

Plaintiff's claim: "The materials shared and downloaded would not be of interest to a child (Id.)" is grossly opinionated. The movie in question lost quite a bit of money. However, it is totally within the range of a child's interest as well as many adults. Besides, nobody really knows who watched what in this country nor anywhere else. Plaintiff makes this claim solely to promote his assertion that in no way would a household have a child download this move (thereby being innocent of wrong doing) since a child would not be interested in it in the first place. That is like saying I'm omniscient and can tell you everything that happened since I know everything. These movie companies try to make a profit, do surveys, market and target children and their parents and sit back while families entertain themselves. I have never seen anything that does not capture a child's attention.

To satisfy the Minute Order of proving that material tracked to the Defendant was playable the Plaintiff would have to find it on one of my computers, confirm it was not already there (I only have "used" computers), show it as being downloaded in it's entirety so that it can even play, and prove that this copy was actually from the film maker and not a camcorder, blue ray, xvid, or any other modified source. These torrent swarm interlocked specs of information are totally unplayable until complete and visibly confirmed by the naked eyed and absolutely nothing can prove otherwise. Even the size of the file would have to match the original otherwise it is somebody else's property and remember: movies are often matched in size especially if sourced from a disc or made to be of one size. Even each piece of the torrent grouped together in a file would need human review just to confirm what is there. Who knows what was uploaded at these torrent sites. Users unwittingly download Trojans, pornography, infected materials, spam, promotions and viruses each and every day. Our emails, back doors, clicking onto anything from any website can lead to a download of any type of material and without itemized review there is no way to tell what is going on in your computer or who is doing activity on a computer. That is why defector and computer expert Edward Snowden hides under a large towel whenever he signs onto a computer: he knows how dangerous a computer is. Oftentimes, invasive programs from

sites continue to grow, take root into a computer, and mask anything done on that machine. This is why our Russian neighbors were able to spoof our U.S. election, Banks are hacked, Uber is corrupted, Social Security, Governments, my computers, credit cards, medical records, S.W.A.T. team incident locations and anything dependent on airways or wires is hacked routinely. The Infiltrators cover their tracks well as exemplified by misidentification of culprits, over a year's review of what happened to our election with no answers, two Uber attacks and nobody knows whether it is Al- Qaeda or my dead Grandmother doing this (yeah, dead people now take wrongful blame for actions all the time).

Forensic review has been postponed in this matter so this threshold is not possible by the Plaintiff. As such, Plaintiff's suit is "dead". I think it was a big mistake for the Plaintiff to threaten me with forensics and his dependency of such necessary actions because it actually disputes everything he and his bogus experts claim to be able to acquire or have acquired. In reality, Plaintiff does not know who is a culprit, if a crime was even committed, or its source or motive. Hard evidence rather than speculation must be used for plausibility. Defendant has no history nor has he distributed anything as claimed by the Plaintiff.

The Plaintiff inundated my email system with the same and additional claims of his case and ongoing requests for me to help him and the FBI solve this matter but also bypassed rule 26 (F) and pursued discovery through intimidation rather than play fairly by the rules. There is a wrongful component to make me rush in these rather uncharted waters so that I operate in fear, face a stringent learning curve, and appear to be ignorant or a simpleton. Such actions mentally fatigue me, instill fear with the possible loss of my job here at the jail, discredit me, and defame my good character. This Plaintiff is indiscriminate in who he pursues and really needs help. The last words singer Keith Cassidy of the Partridge Family said to his estranged Daughter Katie Cassidy were: "So much wasted time". The Plaintiff is wasting everyone's time here. With all due respect, the Plaintiff reminds me of Adolph Hitler's quote: "If you tell a big enough lie and tell it frequently enough, it will be believed."

The Plaintiff has not acted as a professional attorney here in Washington State. The State's governing "Bar" would expect Plaintiff (and his team of lawyers) to be fair and treat their Defendants with respect. The Plaintiff claims to having done over 1,000 infringement cases which I find to be evidence of long term wrong doing towards Defendants (see Exhibit A Plaintiff's email to Defendant). With over three decades as a Correctional Officer, Sergeant level Supervisor experience in Texas Prisons, being a Special Operations Response Team Officer (trained by S.W.A.T.), two years as a West Point Cadet and having served my country for four years in the Army, I too can claim to recognize a wrong doer. The Plaintiff is a wrong doer because these lawsuits are taking advantage of others and the Plaintiff has become sloppy and over confident in his greed and exhibits the character of "champerty". Champerty means: an illegal agreement in which a person with no previous interest in a lawsuit finances it with a view to sharing the disputed property if the suit succeeds. Plaintiff's uses German expert Dr. Simone Richter to explain and illustrate the MaverickEye software which captured the hash mark, computer blip and IP address of Defendants. The doctor's 02 April 2014 paper is not specifically directed at this lawsuit nor is it current or updated to meet the ever changing computer field of today. Passwords and computer code are overcome and hacked routinely like a flu virus upgrading its' defense to antibiotics. Besides, using paid experts to promote Plaintiff's claims is hardly a basis for truth. Dr. Richter makes a living as a professional witness for the German Government and is outdated (no different than the Plaintiff's dragnet profession as an alleged "internet infringement troll"). Today's computer activities and events should not be held to an outmoded standard. Furthermore, Dr. Richter is not likely to travel from

Germany into a Seattle Federal court room for cross examination or even discovery. The RCW 18.165 expects experts doing investigations of Washington residents (and their testimony) to be licensed and bonded by Washington State. Here, unlicensed entities claims for the Plaintiff are illegal and disqualified and not admissible in Washington court. Being unlicensed under RCW 18.165.010 dismisses their evidence by default. Note that under RCW 18.165.020 cited exemptions do not apply. These investigators and experts fall short of court expectations and are out of compliance with RCW 18.165 which protects Washington citizens from abuse by unlicensed investigators as noted in the Fight c Trolls articles. Other articles at Fight c Trolls promoted voluntary dismissals by the Plaintiff regarding the MaverickEye capturing of data per their fail safe (faulty timers) taken in the future for data which had not even occurred yet. Dr. Richter notes his capture of a computer blip is not visible to the human eye. You have to see the data before you know what movie or anything else you are looking at to warrant infringement claims. Also, regarding Plaintiff's claim: "The download of the motion picture was not an isolated infringement, but rather one instance of significant BitTorrent activity in which Defendant's IP address participated during the relevant 3 period (Id. at ¶ 12). All these alleged torrented movies and anything else should not even be part of the Plaintiff's claim since there is no accompanying "blip" as associated as with the Venice movie. These movies are not owned by the Plaintiff or part of an acquisition of rights to copyrighted works, or used by the Plaintiff to represent others to pursue lawsuits. As related to acquisition software the Plaintiff's charts are typed up by the Plaintiff or his staff and are not the byproduct of a MaverickEye printout or other capturing software. Human error and poor transcribing are then introduced and promote inadmissible evidence since they produce false positives. As such, no admissible evidence from German software is usable because of its' inherent technical limitations. How did the Plaintiff acquire this material associated with my IP address and then allegedly acted on it in good faith? There is an ocean of IP addresses which are reused and of no source or association with the Defendant. German software is not a source of evidence in Washington State since they are unlicensed and not admissible in our courts.

Moreover, Plaintiff's using alleged different experts whose signatures and resumes resembled each other to such an extent that they were deemed copied with no such expert even existing (hence the reasoning behind using foreigners) is inadmissible and rather bold. I even found a lawsuit from a female lawyer so similar to Mr. Lowe's (Plaintiff) that I was uncertain and unable to differentiate who actually wrote their respective lawsuits. I admit that sounds vague but it did happen and is plausible. Overall, the Plaintiff is hoping that the judge will not question the background and credentials of his experts and has history of using phony witnesses and experts in prior cases. Note that resumes and histories of the experts fails to meet the Minute Order and cannot merit plausibility until a review in discovery which has yet to occur. Plaintiff's past use of so such experts has led to fraudulence and brought about Defense verdicts. Everything used by the Plaintiff to satisfy the Minute Order is based on repasted information and not original or reviewed to meet the 2017 order date.

The court should recognize the threats, Plaintiff's false pursuits of doing justice by claiming copyright infringement, the bypassing of Rule 26(f) (Exhibit A labeled Mr. Lowe Email), the constant intimidation

and sloppiness of Plaintiff's cut and paste style of formulating claims (see Judge Richard A. Jones Case 2:16-cv-01272-RAJ), ongoing resubmission of Plaintiff's claims, lack of current updated expertise and that using a foreign non U.S. (Germany) 2004 expert amount to a mockery of the court system and are deceptive in nature. This Plaintiff will likely only respond to the court's decrees and admonishment of his actions, fines and counter measures by the Washington Bar after an investigation, pressure by the media and public outcry. There is no measure to the damage done by the Plaintiff to the public. Just the ongoing plots to avoid and ignore deadlines, court no contact orders of pro se defendants and broad stroking claims against Defendants burdens me and promotes this effort (although I am only a pro se layman).

In Prisons and Jails the Plaintiff would be locked down, unable to provoke others that conform to rules (and just want to do their time) and later placed back in the general population once his behavior warranted that. I believe the Plaintiff's disbarment for a length of time and later warranted reinstatement is in order here. I have never enjoyed treating inmates and prisoners to such measures but the history of their behavior warrants such measures and is often all they respond to. The Plaintiff's claim and history of over 1,000 cases shows the Plaintiff is running amok and has nothing to fear. The courts are catching on but it is slow progress for several reasons. To begin with, there is a learning curve to overcome when dealing with difficult and intangible matters regarding computers and airways. These alleged computer experts and program writers resemble statisticians in many ways. By using a statistic an expert can justify any claim or point they are trying to make. Just think of President Reagan using a chalk board, pointer, and graphs to justify his plans of action in this country. Worldwide IP addresses, worldwide movie distribution, a Federal Court system being manipulated by computers and internet court processing exemplify my point that there is much to comprehend. Moreover, the Plaintiff is not afraid of Defendants because most of them are ignorant of how to defend themselves. Plaintiff's claim does not add up that 1,000 of Plaintiff's cases have never shown an innocent person (other than children or neighbors and tenants) who unfortunately are associated with an IP address or one accessible to others. Plaintiff's claims that computers are pass word protectable, WIFI is inaccessible to others and non spoofable and that Defendants must inform the FBI and authorities and even become the Plaintiff's personal police force to righteously seek out copyright infringers is outrageous. Just because I look like a police officer in my jail guard uniform does not permit me to impersonate one. In effect the Plaintiff has repeatedly asked me to break the law which is alarming and very bold. For quite some time the Plaintiff has used the American Federal Court System to partake in this nefarious activity as well.

Plaintiff's claim: "The physical location and layout of Defendant's residence makes it unlikely that his IP address was hijacked by a neighbor or passerby" is false. Really? The Defendant had 37 available WIFI connections when first reviewed in his apartment. Anyone nearby could infiltrate my computer via these entrée points. Also, 763 apartments grouped together and 9 other previously named apartment

complexes, with additional homes and businesses (all within one mile of Defendant) afford piggy backing and spoofing of Defendants WiFi computer connection. Plaintiff's geo location claims only remotely identify Defendant's IP address location and are hardly a reliable source of pinning a crime scene to the Defendant's residence. The computer public is simply too concentrated in my area to isolate anything. Even a culprit's hand held cell phone "passing bye" can attach and spoof itself to Defendant's computer, and then send data (via the phone) to a computer 10,000 miles away without being detected.

Furthermore, the Plaintiff takes no risks of losses because pro se defendants are not usually entitled to monetary compensation in these matters. However, once a demand letter from another attorney is presented to this Plaintiff the results are different. So far, Lee and Hayes PLLC law firm have made the Plaintiff drop at least 12 infringement lawsuits((Fight c Trolls/magazine published April;5, 2017) website:

<https://fightcopyrighttrolls.com/2017/04/05/copyright-troll-david-low-dropped-eleventh-defendant-after-defense-attorney-threatened-to-expose-fraud/>)

because of fears of attorney fees to the Plaintiff, exposure of Plaintiff's scheme thereby arming other victims with legal approaches to defend themselves, the strength of Lee and Hayes arguments, and ways for other attorneys to profit from Plaintiff's exploits (other than averaging about \$350 to \$750 in Defense attorney fees for Defendants going directly to a settlement with no contesting on the Defendant's behalf). In fact, direct uncontested settlement is a travesty given that both Defendant and Plaintiff attorneys profit from these types of lawsuits. Given the Plaintiff's claim to over 1,000 successful lawsuits illustrates how desirable and profitable these lawsuits have become but also what an insult it is that such events occur (I believe Plaintiff meant 1,000 Defendants and 100 lawsuits). Everybody gets a piece of the Defendant's pie (settlement for the Plaintiff) to include the Plaintiff's and Defendant's law firm, the foreign and domestic experts hired by the Plaintiff, the source of the alleged infringed material, and so forth. Society and the tax paying public at large pay a price for the Plaintiff's greed with denying justice in credible matters, impairing trust and usage to anyone using a computer and those affected by computers, ISP agencies, our governments, overall trust in people and so forth (hence the Champerty element).

Characteristic arguments shown in the Fight c Trolls article regarding Lee and Hayes LLC also apply to the Defendant's case, experts, court law, other attorneys and conclusions and outcomes in similar cases (I highly praise their efforts and owe their insight a great deal as follows). Firstly, the Defendant's Internet Provider (IP) address is not a justifiable basis of the Plaintiff's claims. Basically, based largely on this address, the Plaintiff believes Defendant was involved in a bit torrent swarm which reassembled fragments of a movie used to produce an entire film. In reality only a snap shot of IP addresses in the torrent swarm was acquired and then listed as evidence (exhibit b) by the Plaintiff. The Defendant's IP address only shows who pays the Comcast bill (Defendant) and not what may have occurred on one of the Defendant's devices (computers). The Defendant's computers have no trace of the production of the movie: "Once Upon a Time in Venice." which is the alleged movie infringed upon. This movie was not erased but rather never existed. Without discovery (to include forensic examination of devices in defendant's apartment) an IP address is unreliable and seriously weak as a claim. The Plaintiff is not in a position to satisfy the Minute Order's expectation of showing that Defendant's infringed movies are whole and playable since Plaintiff has never even seen my computers let alone play a movie on them.

No proof or plausibility is retrievable at this point for the Plaintiff.

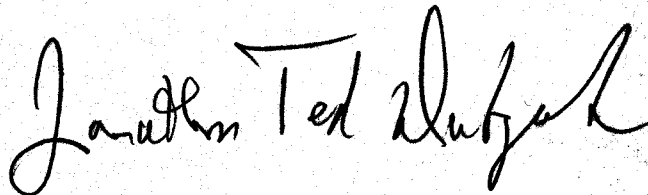
I have spared the courts additional or repeated arguments so that a concise and clearer review of my Claims can occur. Additional insight is available in my first motion to dismiss. Please note that all referenced claims at the Fight c Trolls were directed at Mr. David Lowe (the Plaintiff). Plaintiff is simply playing the odds of this Federally funded "fishing expedition" and regards the occasional dismissals of defendants as bycatch to be thrown back into the ocean.

Should the court find in my favor to dismiss with prejudice I would also seek monetary restitution in this matter. And here I thought I would have an uneventful Christmas.

CONCLUSION:

Please dismiss Plaintiff's lawsuit based on A. The reasoning and facts stated above; B. This response to the Minute Order; and C. Defendant's yet unanswered first Motion to Dismiss with prejudice.

This motion is truthful under penalty of Perjury,

A handwritten signature in black ink that reads "Jonathan Ted Dutczak". The signature is written in a cursive, flowing style.

Jonathan Ted Dutczak
12.14.2017

XFINITY Connect

Jonathandutczak@comcast.net

± Font Size :

RE: Venice PI v. Does, 17-cv-990

From : David Lowe <lowe@lowegrahamjones.com>

Fri, Oct 13, 2017 04:34 PM

Subject : RE: Venice PI v. Does, 17-cv-990

To : JONATHANDUTCZAK <jonathandutczak@comcast.net>

Mr. Dutczak,

Thank you for your email and letter. As previously mentioned, we are happy to discuss the case or work with you informally to identify the responsible party, if you wish. But that if of course not required on your part.

As you know, we represent the Plaintiff, the owner of the infringed copyright in the movie. **We strongly encourage you to consult with an attorney to review your rights in connection with this matter.** If you retain an attorney, please have them contact us. If you continue this discussion with our office directly, we understand that you have opted not to retain an attorney at this time. Again, let us know right away if that status changes.

As previously explained, you have been identified by the Internet Service Provider as the party responsible for the above-identified Internet Protocol ("IP") address at the noted physical address at a time this IP address was being used to distribute the motion picture. We have evidence that someone using your Internet service placed a media file that contains protected film content for the motion picture in a shared folder location enabling others to download copies of this content. Through a direct connection to the infringing computer we have also have obtained the file name used, specifics related to the software used, the file size and additional metadata, all corresponding to the IP address assigned to you at the time the infringing activity occurred. In addition, we have found this same IP address associated with the BitTorrent download of multiple other titles over an extended period of time. With the observed activity associated with your IP address, this type of material is likely tied to an adult(s) at the address who was a permissive user rather than young children.

If you are the responsible party, or wish to take responsibility for infringement that occurred in your household or with your authorization, please let us know. Once we identify the responsible party, we are authorized to engage in a confidential settlement discussion in an effort to resolve the case before extension litigation. All such discussions are protected under court rules related to settlement, namely, as "ER 408" settlement discussions. We have settled many cases amicably and on short order once the responsible party is identified.

If you claim not to be responsible for the infringement, and are willing to voluntarily assist in identifying the responsible party, please let us know. In our experience, given the persistent observed level of BitTorrent activity, it has never been someone outside of the residence, meaning that we can almost always readily find the responsible party. While the subscriber may not be the party responsible for the infringing download/distribution, we find almost invariably that the

responsible party is known to the subscriber, often a family member, friend or houseguest. Often we can ascertain the responsible party based on the demographics of the observed BitTorrent media downloads. If you are willing to voluntarily assist in such investigation, the following information is helpful:

- Who besides you has had access to the IP address since April 2017? This would be someone with very regular access given the observed BitTorrent activity.
- What is the demographic (age, language, ethnicity) of those with access? This helps as we evaluate the other observed BitTorrent activity.
- What computing devices had access? BitTorrent may be used on a desktop, laptop or smartphone, regardless the brand. If necessary, we can have forensic experts examine the device and if it was used for the infringement, locate such evidence, even if the infringer attempts to delete BitTorrent or the media.
- Do you claim to have had an unsecured or "open" WiFi during the relevant period? That would be very surprising. Passwords are the default with Comcast Internet accounts, and to remove them would be in violation of Comcast policy: <http://www.xfinity.com/corporate/customers/policies/highspeedinternetup.html>. Specifically, a customer may not:

resell the Service or otherwise make available to anyone outside the Premises the ability to use the Service (for example, through WiFi or other methods of networking), in whole or in part, directly or indirectly, with the sole exception of your use of Comcast-provided WiFi service in accordance with its then-current terms and policies;

Moreover, customers have an express obligation:

Comcast recommends against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by Comcast and the manufacturer of the applicable file or printer sharing devices. Any files or devices you choose to make available for shared access on a home LAN, for example, should be protected with a strong password or as otherwise appropriate.

You are responsible for your own compliance with this Policy. You are also responsible for any use or misuse of the Service that violates this Policy by anyone else you permit to access the Service (such as a friend, family member, or guest)....

But let us know whether you in fact operated an unsecured, open WiFi, during the time period when this occurred. And if so, when the router was installed, the type of router (and whether from Comcast or the third party), and when the password was removed and replaced.

- What is the physical layout of the residence (where are neighbors located)? This is helpful if there is a claim that others accessed an open WiFi without authorization. If you maintain that someone outside the residence had access and committed the infringement, please identify your neighbors in close proximity to your residence.

You appreciate that it is not as simple as saying "I did not do it." Someone committed the infringement, using your IP address, and continued to use BitTorrent to infringe numerous movies over an extended period of time. We have yet to see any evidence in over 1000 cases where the ISP has provided an incorrect IP address or the infringement did not occur at that IP address. Rather, it always comes down to a question of whether the subscriber or someone to whom they gave or allowed access to the IP address is responsible.

Thank you

David A. Lowe
LOWE GRAHAM JONES
701 Fifth Avenue, Suite 4800 - Seattle, Washington 98104
206.381.3300 Fax: 206.381.3301 LoweGrahamJones.com
DD: 206.381.3303 Cell: 206.335.3303 Lowe@LoweGrahamJones.com

Information in this email message may be privileged, confidential and protected from disclosure. If received in error, please respond and destroy all copies.

From: JONATHANDUTCZAK [mailto:jonathandutczak@comcast.net]
Sent: Thursday, October 12, 2017 9:31 PM
To: David Lowe <lowe@lowegrahamjones.com>
Subject: Re: Venice PI v. Does, 17-cv-990

Hello, I attached a copy of the letter I sent you earlier regarding this case. I don't think I should be on the same time line with the other defendants since I've cooperated with you thus far despite the adversarial nature of our court system. Let me know if anything else is missing or can't be found. I got a copy in the mail today of your request to the courts for a motion for more time. I didn't resign the letter since I don't know how to do computer signatures but rest assured I wrote it, emailed it, and mailed it to you (earlier). Take care, JD.

From: "JONATHANDUTCZAK" <jonathandutczak@comcast.net>
To: "David Lowe" <lowe@lowegrahamjones.com>
Sent: Wednesday, October 11, 2017 8:36:33 AM
Subject: Re: Venice PI v. Does, 17-cv-990

Hello, I think discovery will give us a chance to discuss the case. I will wait to see what the Judge does regarding a dismissal and go from there. Take care, JD.

From: "David Lowe" <lowe@lowegrahamjones.com>
To: jonathandutczak@comcast.net
Cc: "Blake Hoonan" <hoonan@lowegrahamjones.com>
Sent: Monday, October 9, 2017 6:16:28 PM
Subject: Venice PI v. Does, 17-cv-990

Mr. Dutczak,

Please see attach a copy of today's filing.

As an aside, we mentioned therein, I did not receive a copy of an email from you earlier to discuss this case. But if you are still interested in discussing the case, I am happy to do so.

David A. Lowe

LOWE GRAHAM JONES

701 Fifth Avenue, Suite 4800 - Seattle, Washington 98104

206.381.3300 Fax: 206.381.3301 LoweGrahamJones.com

DD: 206.381.3303 Cell: 206.335.3303 Lowe@LoweGrahamJones.com

Information in this email message may be privileged, confidential and protected from disclosure. If received in error, please respond and destroy all copies.

23240 88
Kant wdy: 98031
Stewart T-1 Duties Ave
RUS. B. Apt. J5-204

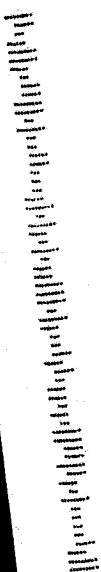
Clerke, United States District Court

US Court House
201B
2 DEC 19 2017

700 Stewart St., Suite
98101

Seattle WA

98101-444285



CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY

FILED
LIBERO
RECEIVED
MAIL
2017

16 DEC 2017

SEATTLE

